UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,280	02/04/2002	Mark J. McArdle	01.239.01	9739

7590 11/15/2005

ZILKA-KOTAB PC
PO Box 721120
San Jose, CA 95172-1120

EXAMINER	
HA, LEYNNA A	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/068,280	MCARDLE ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-47 have been amended and new claims 27-51 are now pending.

2. This is a FINAL rejection.

Claim Objections

35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 51 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 51 is a newly added claim wherein includes the new limitation of "heuristic rule includes information associated with an active networked application making a new connection never previously made". The limitation of claim 51 cannot be found for any support was neither in the specification nor was this limitation a clarification to the

originally claimed language. Therefore, claim 51 is objected to because this claims benefit to claim 1 that is not being rejected under 35 U.S.C. 112, first paragraph.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 14-26, 28-40, 42-48, and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (5,987,611) and in further view of Kaler, et al. (US 6,671,829).

As per claim 1:

Freund teaches a computerized method comprising:

determining an active networked application; **[col.10, lines 31-44 and col.30, lines 13-15]**

filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application **[col.4, lines 65-67**

and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and **[col.5, lines 46-59 and col.8, lines 45-52]**

evaluating network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of

Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 2: See Freund on col.4, lines 51-62; discusses detecting when the active networked application becomes inactive and re-filtering the set of intrusion rules.

As per claim 3: See Freund on col.13, lines 20-22; discusses monitoring network connection terminations.

As per claim 4: See Freund on col.13, lines 20-22; discusses monitoring application terminations.

As per claim 5: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

As per claim 6: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses continuing the evaluating of network traffic if no networked application is active.

As per claim 7: See Freund on col.10, lines 31-44 and col.30, lines 13-15; discusses detecting when a network connection for an active application is initiated.

As per claim 8: See Freund on col.5, lines 46-59 and col.13, lines 50-56; discusses marking an intrusion rule corresponding to the active networked application.

As per claim 9: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses extracting the subset of rules into an optimized set of rules.

As per claim 10: See Freund on col.12, lines 3-5; discusses analyzing network traffic on a port specified in the subset of rules.

As per claim 11: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses analyzing network traffic for a protocol specified in the subset of rules.

As per claim 12: See Freund on col.13, lines 15-22; discusses discarding network traffic that satisfies at least one of the subset of rules and reporting an intrusion attempt.

As per claim 14: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 15:

discusses a computer-readable medium having executable instructions to cause a computer to perform a method comprising:

determining an active networked application; **[col.10, lines 31-44 and col.30, lines 13-15]**

filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application **[col.4, lines 65-67 and col.5, lines 39-43]**, where the subset of the intrusion rules corresponding to the active networked application are capable of being

used for evaluating intrusions that target the corresponding active networked application; and **[col.5, lines 46-59 and col.8, lines 45-52]**

evaluating network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the

information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 16: See Freund on col.4, lines 51-62; discusses detecting when the active networked application becomes inactive, and re-filtering the set of intrusion rules.

As per claim 17: See Freund on col.13, lines 20-22; discusses monitoring network connection terminations.

As per claim 18: See Freund on col.13, lines 20-22; discusses the detecting comprises:

monitoring application terminations.

As per claim 19: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses detecting when no networked application is active', and suspending the evaluating of network traffic until a network application is active.

As per claim 20: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses continuing the evaluating of network traffic if no networked application is active.

As per claim 21: See Freund on col.10, lines 31-44 and col.30, lines 13-15; discusses detecting when an active application initiates a network connection.

As per claim 22: See Freund on col.5, lines 46-59 and col.13, lines 50-56; discusses marking an intrusion rule corresponding to the active networked applicaticm.

As per claim 23: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses extracting the subset of rules into an optimized set of rules.

As per claim 24: See Freund on col.12, lines 3-5; discusses analyzing network traffic on a port specified in the subset of rules.

As per claim 25: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses analyzing network traffic for a protocol specified in the subset of rules.

As per claim 26: See Freund on col.13, lines 15-22; discusses discarding network traffic that satisfies at least one of the subset of rules; and reporting an intrusion attempt.

As per claim 28: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 29:

discusses a system comprising:

a processor coupled to a memory through a bus; and **[col.7, lines 40-51]**

an intrusion prevention process executed from the memory by the processor to cause the processor to determine an active networked application**[col.10, lines 31-44 and col.30, lines 13-15]**, to filter a set of intrusion rules to create a subset of rules corresponding to the active networked application **[col.4, lines 65-67 and col.5, lines 39-43]**, where the subset of the intrusion rules corresponding to the active networked

application are capable of being used for evaluating intrusions that target the corresponding active networked application **[col.5, lines 46-59 and col.8, lines 45-52]** and to evaluate network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the

information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 30: See Freund on col.4, lines 51-62; discusses the intrusion prevention process further causes the processor to detect when the active networked application becomes inactive, and to re-filter the set of intrusion rules.

As per claim 31: See col., lines ; discusses the intrusion prevention process further causes the processor to monitor network connection terminations in detecting when the active networked application becomes inactive.

As per claim 32: See col., lines ; discusses the intrusion prevention process further causes the processor to monitor application terminations in detecting when the active networked application becomes inactive.

As per claim 33: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses the intrusion prevention process further causes the processor to detect when no networked application is active, and to suspend evaluating network traffic until a network application is active.

As per claim 34: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses the intrusion prevention process further causes the processor to further tilter the intrusion rules based on an operating system and to continue evaluating network traffic if no networked application is active.

As per claim 35: See Freund on col.10, lines 31-44 and col.30, lines 13-15; discusses the intrusion prevention process further causes the processor to detect when an active application initiates a network connection in determining an active networked application.

As per claim 36: See Freund on col.5, lines 46-59 and col.13, lines 50-56; discusses the intrusion prevention process further causes the processor to mark an intrusion rule corresponding to the active networked application in filtering the set of intrusion rules.

As per claim 37: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the intrusion prevention process further causes the processor to extract the subset of rules into an optimized set of rules in filtering the set of intrusion rules.

As per claim 38: See Freund on col.12, lines 3-5; discusses the intrusion prevention process further causes the processor to analyze network traffic on a port specified in the subset of rules in evaluating the network traffic.

As per claim 39: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the intrusion prevention process further causes the processor to analyze network traffic for a protocol specified in the subset of rules in evaluating the network traffic.

As per claim 40: See Freund on col.13, lines 15-22; discusses the intrusion prevention process further causes the processor to discard

network traffic that satisfies at least one of the subset of rules, and to report an intrusion attempt in evaluating the network traffic.

As per claim 42: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 43:

discusses an apparatus comprising:

means for determining when an active application becomes an active networked application; **[col.10, lines 31-44 and col.30, lines 13-15]**

means for filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application **[col.4, lines 65-67 and col.5, lines 39-43]**, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and **[col.5, lines 46-59 and col.8, lines 45-52]**

means for evaluating coupled to the means for filtering to evaluate network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 44: See Freund on col.4, lines 51-62; discusses the means for determining further detects when the active networked application becomes inactive and the means for filtering further re-filters the set of intrusion rules when the active networked application becomes inactive.

As per claim 45: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses the means for determining further detects when no networked application is active and the means for evaluating further suspends the evaluation of network traffic until the means for determining determines a networked application is active.

As per claim 46: See Freund on col.13, lines 50-56 and col.26, lines 55-58; discusses the means for filtering further filters the intrusion rules corresponding to an operating system and the means for evaluating continues the evaluation of network traffic when the means for determining determines no networked application is active.

As per claim 47: See Freund on col.13, lines 15-22; discusses means for discarding network traffic that satisfies at least one of the subset of rules; and means for reporting an intrusion attempt.

As per claim 48: See Freund on col.11, line 56 – col.12, line 17 and col.13, lines 13-22; discusses intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol.

As per claim 50: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 51: See Freund on col.10, lines 31-44 and col.30, lines 13-15 and col.13, lines 34-42 and col.5, lines 39-43; discusses the heuristic rule includes information associated with an active networked application making a new connection never previously made.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 13, 27, 41, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund and Kaler, et al, and further in view of Official Notice.

As per claim 13:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and

analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

As per claim 27:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding

to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for

identifying infected programs from another signature in order to provide a solution or antivirus program.

As per claim 41:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A

signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

As per claim 49:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of

modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

Primary Examiner
Art Unit 2135